impermissible values taken by the control fields in the respective data buffers with a corresponding permissible value.

REMARKS

Upon entry of this amendment, claims 1-17 are pending. By the present amendment, claims 21-23 have been canceled without prejudice, and claims 1, 2, 4, 5, 8-10 and 13-16 have been amended for clarity.

The rejection of claims 1-17 and 21-23 under 35 U.S.C. § 103(a) over Clarke et al. (U.S. Patent No. 5,550,914, hereinafter "Clarke") in view of Weisser (WO 95/35633) is respectfully traversed. Without acquiescing in the rejection, claims 21-23 have been canceled without prejudice and claims 1, 2, 4, 5, 8-10 and 13-16 have been amended for clarity. Accordingly, the rejection will be discussed with respect to the pending and amended claims.

As discussed in previous responses, Clarke is directed to a communications signalling network apparatus. Clarke discloses a message interceptor that is interposed in a link of a communications signalling network such as an SS7 network. The interceptor purportedly separately maintains the link level protocols on the two portions of the link with which it interfaces. Message data is transferred across between the link portions by a transfer circuit of the interceptor. In the course of this transfer, the nature of the data is checked by a selective action

control circuit against selection criteria held in a store. If a selection criteria is met, the control circuit acts to suppress or modify the data.

Significantly, there is no teaching or suggestion anywhere in Clarke of the specifically recited comparison and overwrite features of the claimed invention. In particular, the selective action control circuit of Clarke acts to *suppress* (*i.e.*, block) the transfer of data contents onward when the data includes impermissible values (*see*, *e.g.*, col. 8, lines 36-56, especially lines 49-56). This teaching of Clarke is the *opposite* of the claimed features of comparing a value stored in the control field with a set of permissible values and if the value is determined to be impermissible, overwriting (not blocking) the impermissible value with a permissible value.

The data modification circuit of Clarke does not overwrite the data of the control field or take any corrective action as set forth in the claims. Instead, and quite to the contrary, the data modification modifies *permissible* data, it does not overwrite *impermissible* values in the control field with a value from a subset of a plurality of possible values or correct it. The purpose of the data modification circuit of Clarke is to effect modification of the *permissible* MSU data transferred out of the register to the buffer. Examples of such data modification include encryption or decryption of the message, etc. (*see*, *e.g.*, col. 11, lines 10-16).

In summary, Clarke discloses either *blocking* the message entirely if it is impermissible, or, alternatively, modifying a *permissible* message in a complex manner if the message requires some processing to be carried out on it (*e.g.*, to perform encryption or decryption of the message). It is important to note that the modification of data only occurs if the data has been deemed *permissible*. There is no teaching or suggestion anywhere in Clarke of modifying or correcting *impermissible* data. In complete contrast to the claimed invention, the only action taken according to Clarke upon the detection of impermissible data is to block such data from being transferred. The impermissible data of Clarke is not overwritten or corrected, as specifically recited in the claims. The modification of Clarke is only selective in that not all data transferred by the transfer circuit will require modification (*see*, *e.g.*, col. 10, lines 45-48). Accordingly, Clarke is inapplicable to the claimed invention.

It is respectfully submitted that Weisser fails to overcome the fundamental deficiencies noted above with respect to Clarke. In particular, there is no teaching or suggestion in Weisser of the specifically recited features of comparing a value stored in the control field with a set of permissible values and if the value is determined to be impermissible, overwriting (not blocking) the impermissible value with a permissible value.

Specifically, in the system disclosed by Weisser, there are two distinct network elements (26' and 20') involved in screening messages coming from or going to an external network element (47). One of these elements is the Service

Transfer Point 20', which acts as the main gatekeeper, while the other element, Service Control Point 26', is a more powerful device that only looks at messages from outside the network that have already made it past the gatekeeper STP 20'.

The STP 20' examines the incoming message, and if it finds that the message is impermissible, it rejects the message (*see, e.g.*, Page 15, first paragraph, and paragraph bridging pages 24 and 25). There is no suggestion anywhere in Weisser of the STP 20' overwriting this impermissible data with permissible data and then allowing the packet to proceed for further processing.

The function of the SCP 26' is fundamentally different from that of the STP 20'. The main responsibility of the SCP 26' is altering information contained in the packets *leaving* the network so as to obscure the internal workings of the network from an outside party. With respect to incoming messages (that have already passed the STP 20'), the SCP 26' checks whether their transaction numbers match up with ones allocated previously by the SCP 26'. Significantly, the SCP 26' is not directly connected to any external sources, and is thus inapplicable to any of the claims. In particular, the SCP 26' is not connected to multiple sources of external signals. Instead, there is only one connection from which it is receiving all of the signals that might have arrived from an external source via the STP 20'. Thus, any overwriting the SCP 26' may perform is not the overwriting set forth in the claimed invention. In other words, any overwriting performed by the SCP 26' is not of impermissible data being overwritten by permissible data, but rather translating between obscure uninformative data for transmission *outside* of

the network and informative data used inside the network. This is entirely inapposite to the claimed invention.

Therefore, it is respectfully submitted that Weisser does not overcome the fundamental deficiencies noted above with respect to Clarke. Thus, even if, *arguendo*, the combination of Clarke and Weisser were proper, the combination nevertheless fails to render the claimed invention obvious. In particular, neither reference, either singly or in combination, discloses, teaches or suggests the claimed feature of comparing a value stored in the control field with a set of permissible values and if the value is determined to be impermissible, overwriting (not blocking) the impermissible value with a permissible value. Accordingly, reconsideration and withdrawal of the rejection are respectfully requested.

In view of the foregoing, it is respectfully submitted that the entire application is in condition for allowance. Favorable reconsideration of the application and prompt allowance of the claims are earnestly solicited.

Should the Examiner deem that further issues require resolution prior to allowance, the Examiner is invited to contact the undersigned attorney of record at the telephone number set forth below.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
Updeep S. Gill
Reg. No. 37,334

USG:dbp
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

MARKED-UP VERSION OF AMENDED CLAIMS

1. (*Thrice Amended*) A method of operating a node in a communications network, which node is in use connected to signal sources external to the communications network via respectively corresponding links, the method comprising:

a) receiving from [a] respective signal [source] sources signals which include a control field, which control field takes one of a plurality of possible values, and the subsequent handling of the said signal by the network being controlled according to the value of the control field;

b) within a lower level of a messaging protocol, and prior to the processing of the signal by higher level functions, comparing the value stored in the control field with a set of permissible values, said set being a restricted subset of the plurality of possible values, to determine if the value is a permissible or impermissible value, and if the value is determined to be impermissible, overwriting the control field with a permissible value [from a restricted subset of the plurality of possible values]; and

c) subsequently processing the signal in the network in dependence upon the said permissible value from the restricted subset of the plurality of possible values.

2. (*Thrice Amended*) A method of operating a communications network comprising:

a) communicating control signals between nodes of the network via respectively corresponding links which control signals conform to a predetermined signalling protocol;

b) at one of the said nodes, receiving from a signal source external to the network signals conforming to the said predetermined protocol and including a control field, which control field takes one of a plurality of possible values;

c) within said lower level of a messaging protocol running on the node, and prior to the processing of the signal by higher level functions running on the node, comparing the value stored in the control field with a set of permissible values, said set being a restricted subset of the plurality of possible values, to determine if the value is a permissible or impermissible value, and if the value is determined to be impermissible, overwriting the control field with a permissible value [from a restricted subset of the plurality of possible values]; and

d) subsequently processing the signal in the network in dependence upon the said permissible value from the restricted subset of the plurality of possible values.

4. (*Twice Amended*) A method according to claim 1, in which the said control field is a routing control field, and the overwriting of the routing control field with a [predetermined] permissible value [in step (b)] limits the

routing of signals to or from the external [source] sources to [part] only part of the communications network.

5. (*Amended*) A method according to claim 4, in which the routing of signals to or from the external [source] sources is limited to a point-to-point connection between the respective external source and the node.

8. (*Twice Amended*) A node suitable for connection in a communications network and comprising:

a) a network interface for connection to the communications network;

b) a signal interface for connection to a signal source external to the communications network via respectively corresponding links;

c) means connected to the signal interface for [overwriting] comparing, within a lower level of a messaging protocol, the value stored in the control field with a set of permissible values, said set being a restricted subset of the plurality of possible values, to determine if the value is a permissible or impermissible value, and if the value is determined to be impermissible, overwriting the control field with a permissible value [a control field in a signal received via the signal interface from the signal source with one of a subset of predetermined values]; and

d) signal processing means for processing the said signal in dependence upon the [said one of a subset of predetermined values] permissible value adopted by the control field.

9. (*Amended*) A node according to claim 8, in which the said means for [overwriting] comparing is [are] located within a data link layer interface, which data link layer interface is arranged to respond to service requests [request] from network layer functions of the node and to issue service requests to the communications network.

10. (*Twice Amended*) A node according to claim 8, in which the signal processing means [are] is arranged to route the signal in dependence upon the value of the said control field.

13. (*Thrice Amended*) A method of operating a node in a communications network, which node is in use connected to [a] signal [source] sources external to the communications network via respectively corresponding links, the method comprising:

a) receiving from one of the said signal [source] sources signals which include a control field, which control field takes one of a plurality of possible

values, and the subsequent handling of the said signal by the network being controlled according to the value of the control field;

b) within a lower level of a messaging protocol running on the node, and prior to the processing of the signal by higher level functions running on the node, comparing the value stored in the control field with a set of permissible values, which set includes a restricted subset of the plurality of possible values, to determine if the value is a permissible or an impermissible value, and in the event that the value is determined to be an impermissible value, overwriting the control field [at a low level process] with a permissible value [from a restricted subset of the plurality of possible values]; and

c) subsequently processing the signal in the network in dependence upon the [said] permissible value [from the restricted subset of the plurality of possible values] stored in the control field.

14. (*Twice Amended*) A method of operating a communications network comprising:

a) communicating control signals between nodes of the network via respectively corresponding links, which control signals conform to a predetermined signalling protocol;

b) at one of the said nodes, receiving at a low level process from a signal source external to the network signals conforming to the said predetermined

protocol and including a control field, which control field takes one of a plurality of possible values;

c) within a lower level of a messaging protocol running on the node, and prior to the processing of the signal by higher level functions running on the node, comparing the value stored in the control field with a set of permissible values, which set includes a restricted subset of the plurality of possible values, to determine if the value is a permissible or an impermissible value, and in the event that the value is determined to be an impermissible value, overwriting [at a low level process] the control field with a permissible value [from a restricted subset of the plurality of possible values]; and

d) subsequently processing the signal in the network in dependence upon the [said] permissible value [from the restricted subset of the plurality of possible values] stored in the control field.

15. (*Thrice Amended*) A method of operating a node in a communications network, which node is in use connected to a signal source external to the communications network via respectively corresponding links, the node including a data link layer interface arranged to respond to service [request] requests from network layer functions of the node and to issue service requests to the communications network, the method comprising:

a) receiving from the said signal source signals which include a control field, which control field takes one of a plurality of possible values, and the subsequent handling of the said signal by the network being controlled according to the value of the control field;

b) within the data link layer interface, and prior to the processing of the signal by higher level functions running on the node, comparing the value stored in the control field with a set of permissible values, which set includes a restricted subset of the plurality of possible values, to determine if the value is a permissible or an impermissible value and, in the event that the value is determined to be an impermissible value, [at a low level process] overwriting the control field with a permissible value [from a restricted subset of the plurality of possible values]; and

c) subsequently processing the signal in the network in dependence upon the [said] permissible value [from the restricted subset of the plurality of possible values] taken by the control field.

16. (*Twice Amended*) A method according to claim 1 [including] comprising writing control field data received on each of a plurality of signalling links into respective signalling link data buffers, and, when required, overwriting [the] impermissible values taken by the control fields in the respective data buffers with [the said] a corresponding permissible value.